UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

Information associated with holidatstyle43@yahoo.com that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014

Case No. 18-M-1248

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

SEE ATTACHMENT A

located in the Eastern District of Wisconsin, there is now concealed:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim P. 41(c) is:

- ■ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of:

Title 18, U.S.C. §1591, Sex Trafficking of children or by force, fraud or coercions; and §1952, Use of facility in interstate commerce to carry on or distribute the proceeds of prostitution activity.

The application is based on these facts: See attached affidavit.

Applicant's signature

FBI Special Agent Heather Wright

Printed Name and Title

Sworn to before me and signed in my presence:

Date: 4/19/18

Judge's signature

City and State: Milwaukee, Wisconsin

William E. Duffin, U.S. Magistrate Judge

Printed Name and Title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT APPLICATIONS

I, Heather Wright, being first duly sworn, hereby depose and state as follows:

I. Agent Background & Experience.

1. I am a Special Agent with the Federal Bureau of Investigation, and I have been so employed since July 2010. I am assigned to the Wisconsin Human Trafficking Task Force, which investigates the illegal trafficking of persons for labor and commercial sex acts. I gained experience in such investigations through prior cases, formal training, and in consultation with local, state, and federal law enforcement colleagues. Before joining the FBI, I worked in the pharmaceutical manufacturing industry as a Programmer Analyst for web applications and an Automation Engineer.

2. The facts in this affidavit come from my personal observations, my training and experience, information obtained from witnesses, and information reported to me by other law enforcement officers, all of whom I believe to be truthful and reliable. In this affidavit, "case agents" refers to the federal and local law enforcement officers who have participated in this investigation and with whom I have had regular contact regarding this investigation.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested search warrants and does not set forth all of my knowledge about this matter.

II. Purpose of Affidavit.

4. I make this affidavit in support of applications for the following search warrants under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), requiring the identified entity to disclose, and authorizing the government to search, the information described below and in Attachments A and B to each application:

a. A warrant requiring **Apple Inc.** ("Apple") to disclose records and other information, including the contents of communications, associated with

the Apple ID **holidatstyle43@yahoo.com**, stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, California; and

b. A warrant requiring **Verizon Wireless** to disclose records and other information, including the contents of communications, associated with the phone number **(262) 388-7485**, stored at premises owned, maintained, controlled, or operated by Verizon Wireless, a company headquartered at 180 Washington Valley Road, Bedminster, New Jersey.

5. Based on the facts set forth in this affidavit, there is probable cause to believe that the information described in Attachment A to each application contains evidence of violations of Title 18, United States Code, Section 1591 (sex trafficking by force, fraud, or coercion), and Title 18, United States Code, Section 1952 (use of facility in interstate commerce to carry on or distribute the proceeds of prostitution activity), as described in Attachment B to each application.

III. Probable Cause.

A. Introduction.

6. Case agents have been investigating Christopher L. Childs, Jennifer E. Campbell, and others for the above offenses since May 2017. On March 28, 2018, I applied for and obtained a federal criminal complaint charging Childs with sex trafficking. On April 10, 2018, a grand jury indicted Childs on one count of conspiracy to engage in sex trafficking (beginning before 2009 and continuing into 2018) and two counts of sex trafficking by force fraud and coercion.

7. The investigation is continuing as to additional victims, including one or more minors. The investigation also is continuing as to Campbell's conduct.

B. Information provided by Victim 1.

8. On May 16, 2017, Victim 1 reported to local law enforcement that from October 31, 2015, through May 15, 2017, Childs had coerced her to engage in commercial sexual

activity. On May 19, 2017, other agents and I interviewed Victim 1. Victim 1 described how Childs recruited and ultimately convinced her to dance and perform sex acts on his behalf. Victim 1 described how Childs demanded that she provide all money earned from dancing, sex acts, and her legitimate job as a certified nursing assistant (CNA) to him.

9. Victim 1 also explained that Childs had her take out a loan in order to buy Childs a truck. In approximately January 2016, Victim 1 moved into the apartment where she resided until she left Childs on May 15, 2017. At that time, Childs had her take a $4,500 title loan out on the truck to pay her rent and security deposit. Soon after Victim 1 left Childs, he defaulted on the truck loan, and the truck was repossessed.

10. Victim 1 explained that by February 2016, she had stopped working as a CNA and was stripping and prostituting for Childs full time. After Victim 1 began working for Childs on a full time basis, Childs became physically and sexually abusive to her. Victim 1 explained that the first beating came after she made a negative comment about Jennifer Campbell, whom Victim 1 knew as Childs' "bottom" or most-trusted prostitute. Victim 1 then described a series of beatings and acts of violence by Childs to punish Victim 1 and enforce his rules between July 2016 and May 2017.

11. Victim 1 further reported that she had witnessed Childs beat Victim 2 on a number of occasions, usually for talking back to Childs. Victim 1 also observed that Victim 2 often had fresh injuries. On one occasion, Victim 2 and Childs were fighting and Victim 2 picked up her toddler in fear that Childs's was physically assault her. Victim 2 told Childs that he could not hit her while she had her daughter in her arms. Childs took the child from Victim 2, handed the child to Victim 1, and took Victim 2 into the bathroom. Victim 1 then heard Victim 2 screaming. The following day, on the way to the strip club, Victim 1 observed bruises all over

Victim 2. Victim 2 told Victim 1 that Childs had never beaten Victim 2 so badly before. I later interviewed Victim 2 who described this same beating in detail.

12. Victim 1 explained that Childs controlled every aspect of her life, including what Victim 1 ate. Victim 1 also described Childs' rules when working at strip clubs and performing prostitution dates. For example, Childs told Victim 1 and Victim 2: (a) never to look a black male in the eye; (b) never to give an older black male more than 5-10 minutes of time if they were not making money; (c) never to buy their own drinks; (d) to always offer "extras" at additional charge to potential customers even if they did not ask for them; and (e) to turn over all of the proceeds to Childs. Violations of these rules were met with severe punishments.

13. Victim 1 explained that the majority of her prostitution dates occurred at TNT and the Hardware Store, which are strip clubs located in Dodge County, Wisconsin. Victim 1 reported that Childs had a good relationship with the club managers and would call them to verify how many dates and how much money Victim 1 made. At the end of every night, Childs required Victim 1 and Victim 2 to bring him all of the money that they made. Initially, Victim 1 had to drop the money off at Childs' residence on the way home from the strip club. The managers would provide payment to Victim 1 and Victim 2 in sealed envelopes. Childs later installed a safe in an apartment Victim 1 and Victim 2 shared, and they were to drop their envelopes through a slot into the safe. Childs had a key to the apartment and could pick up the money whenever he wished.

14. If any of the money was missing, Childs would punish Victim 1 and Victim 2. Punishments involved either physical abuse or sexual torture. For example, Childs punished Victim 1 by ordering her place various items, including a hot curling iron, kitchen brush with bristles, or knitting needles, in her vagina.

15. Victim 1 reported that even when Childs was not present, he would randomly contact Victim 1, demand that she engage in sex acts or torture herself, and send Childs videos or photos as proof. If Victim 1 refused, Childs would beat her when he next saw her.

16. Victim 1 reported that Childs and Campbell lived in Hartford, Wisconsin, at a residence owned by S.B., a prostitution customer of Campbell's. Victim 1 reported that Childs instructed Victim 1 to learn from Campbell regarding the types of prostitution dates to perform and to have her approve the prices to charge. Childs also instructed Victim 1 to text or call him before and after each prostitution date.

17. Victim 1 reported that she and Campbell traveled to the Chicken Ranch, a brothel located in Nevada, to earn money for Childs. Campbell instructed Victim 1 on the sex acts occurring at the brothel and acted as a "spy" for Childs 1 to keep tabs on Victim 1.

18. Victim 1 reported that Campbell also was working at the Geisha House, a massage parlor operating as a brothel in Madison. In February 2017, Campbell and Victim 1 filled out applications to work at the Geisha House. The owner explained that they could keep any money for "extras," while the owner would retain the price of the massage. The owner told Campbell and Victim 1 that if the police came, Campbell and Victim 1 would be on their own. Ultimately, only Campbell was hired. Childs told Victim 1 that Campbell was making $500 to $1300 a day at the Geisha House.

19. In early 2017, Victim 1 began to consider leaving Childs. In May 2017, after a customer had been extremely rough with her, Victim 1 left the Hardware Store early. When she called Childs to report this, she was crying. Because Childs had a rule that Victim 1 was not allowed to show weakness by crying, he became angry. After that, Victim 1 stopped taking Childs' calls.

20. On May 14, 2017, Victim 1 was at her mother's house to celebrate Mother's Day. Childs called Victim 1 and asked where she was. Victim 1 had sent some friends messages on Facebook about wanting to leave Childs. Victim 1 believed that Childs had logged into her account and read the messages. The next day, Victim 1 drank shots of alcohol at the Hardware Store and left early. Childs contacted the club, looking for Victim 1. Shortly thereafter, Childs showed up at Victim 1's apartment and hit Victim 1 on her arm and her neck. He grabbed her Victim 1 by the throat and threw her against the wall. Childs also grabbed Victim 1's cellular phone and began deleting videos, photos and text messages from the phone that would incriminate him.

21. Following this incident, Victim 1 stopped working for Childs and obtained a new job as a CNA. Childs, however, continued to contact Victim 1 regularly by phone, and Victim 1 allowed the contact due to fear that Childs would retaliate if she broke off communication. Over time, Childs began to reassert control over Victim 1. Childs began making demands, such as that Victim 1 send him pictures of herself. On February 14, 2018, Childs told Victim 1 that he needed to "borrow" $400. Childs told Victim 1 that if she did not give him the money, "things were going to get ugly." Over time, Childs began to refer to Victim 1's paycheck from her CNA job as "our check."

22. On March 23, 2018, Childs texted Victim 1, indicating that they needed to talk. When Victim 1 asked what they needed to talk about, Childs replied, "About money; I'm gonna start controlling it again." In a call later that day, Childs told Victim 1 that he needed Victim 1's debit card to make him feel better.

C. Information provided by Victim 2.

23. On March 30, 2018, and on April 10, 2018, case agents interviewed Victim 2. Victim 2 fully corroborated the information provided by Victim 1 regarding how Childs treated his victims and Childs' rules. Victim 2 described how Childs controlled what she ate, what she could drink, and even when she could use the bathroom. Victim 2 also described how starting in September 2015, Childs had forced to perform commercial sex acts at the Hardware Store and TNT and provided details of instances in which Childs beat her and urinated on her for violating his rules.

D. Corroboration of Victim 1 & Victim 2.

24. Law enforcement corroborated the information provided by Victim 1 and 2. For example, case agents verified the existence of the safe placed by Childs at Victim 1's residence. Case agents also obtained police reports dating back to 2009 in which a domestic violence victim reported that Childs was her "pimp." Case agents also obtained records documenting Victim 1's ownership of the vehicle Childs had placed in her name. Case agents also confirmed through public records that S.B. owns the residence at which Childs and Campbell lived in Hartford. In addition, case agents interviewed S.B., who acknowledged that he has been a regular customer of Campbell's for years and had paid her for sex at TNT, the Hardware Store and the Geisha House.

25. Case agents also obtained records from the Chicken Ranch. The records verified that Campbell worked at that brothel on 10 occasions (totaling approximately 33 weeks between July 6, 2014, and March 21, 2016). The records also confirmed that Victim 1 and Campbell worked on overlapping dates on at least one occasion.

26. Victim 1's information also was corroborated by a conversation with Campbell on December 20, 2016, which Victim 1 recorded at Childs' behest. In that recording, Campbell

laments that her children are now old enough to realize that Childs is a pimp and that she works for him. Campbell regrets that her children constantly witnessed Childs physically abusing her and knew that he cheats on Campbell with the other women who work for him. Campbell feared that her children would become violent like Childs.

27. Information obtained through the execution of search warrants for Facebook records also corroborated Victim 1 and Victim 2. For example, Childs received and sent photos or memes related to being a pimp, engaged in conversations in which he confirms that he takes all of the money earned by his victims, discussed his rules, and sought to recruit women. In March 2014, he bragged in a Facebook post that he had been a pimp for 18 years.

28. The Facebook materials also include direct communications between Childs and Victim 1 and Victim 2. Two examples illustrate the content of the Facebook materials:

a. In a conversation-taking place on August 6, 2016, Childs directed Victim 1 to torture herself as "punishment." Childs told Victim 1 that she must sleep with a bottle inserted into her rectum for 3 weeks and that she had a week to force her fist into her vagina. When Victim 1 told Childs that trying to stick the bottle into her rectum "hurts so bad," Childs responded, "I want it to hurt."

b. In a conversation on November 13, 2015, Victim 2 stated that she wanted to return Childs' phone and "be done" working for him. Childs told her, "You're not done" and "Don't make me come find you." Childs reminded her that he would never let her leave, noting that he put too much "work and effort into you to let you just walk away." Childs stated that Victim 2 could not become a "lost investment" and added, "I'm not gonna let you fuck up my plans." When Victim 2 countered that there was nothing Childs could do, Childs replied, "There's a lot I can do and if you'd like me to show you I will." Childs further warned Victim 2 not to "underestimate" what he would do to her. Childs then asked if Victim 2 wanted to leave because Victim 1 had begun working for him. Victim 2 begged Childs to "replace" her with Victim 1, allow her to return Childs' property, and let her leave "peacefully." Childs stated that he was "getting real pissed off" and told Victim 2, "You are my property."

E. Victim 3.

29. On January 5, 2018, Victim 1 reported that Childs had recruited Victim 3. Victim 1 then spoke directly to Victim 3, with whom she was already acquainted. On January 25, 2018, Victim 1 reported that Victim 3 did not like the way Childs was treating her and that Childs made her call him "Daddy," a term indicating he was her pimp.

30. During the night of January 27, 2018, Victim 1 called me, noticeably upset. Victim 1 explained that Victim 3 was distraught because "Scottie" had called Childs and accused Victim 3 of causing problems with other dancers and the owner of the Hardware Store. I have verified through phone records that Scottie called Childs as reported by Victim 1.

31. During their call on January 27, 2018, Victim 3 stated that Childs was sending Campbell to pick up Victim 3 from the Hardware Store. Victim 3 told Victim 1 that Scottie had called Childs because he wanted Victim 3 to go on stage, but she refused. Victim 3 explained that she was exhausted because Childs was making her work 15-hour days. Following her phone call with Victim 3, Victim 1 spoke to Childs. Childs said that he was going to make Victim 3 stay at the Hardware Store and work. Childs told Victim 1, "I know the bitch is tired, but she needs to make that dough."

32. Following my January 27, 2018, telephone call with Victim 1, I contacted the Dodge County Sheriff's Office. Shortly thereafter, a Dodge County Deputy conducted a traffic stop on Childs' vehicle. Victim 3 was identified as Childs' passenger.

33. On February 3, 2018, I again spoke with Victim 1. Victim 1 reported that Childs had told her that Victim 3 had been drunk at a restaurant in Hartford and told customers that because she gave all her money to Childs, she did not have money for her meal. Childs told Victim 1 that he was going to "kill this bitch." When Victim 1 had finished speaking with

Childs, fearing for Victim 3's safety, Victim 1 anonymously called the police. I have confirmed these events with Hartford Police Detective Richard Thickens, who provided reports regarding the incident at the restaurant. When police spoke with Childs that evening, he acknowledged that Victim 3's room at the Super 8 in Hartford was under his name. Case agents also obtained records confirming that Childs had rented rooms at the Super 8 from January 19 through January 27 and from January 30 through February 4, 2018.

34. On February 5, 2018, I spoke with Victim 1. Victim 1 reported that Childs and Victim 3 were at a hotel in Madison and that Victim 3 was working at the Geisha House with Campbell. Childs told Victim 1 that he was watching Victim 3 at all times. Childs indicated that he had taken Victim 3's phone. Childs also told Victim 1 that he had changed his phone number to avoid law enforcement detection.

35. Later that same day, I again spoke with Victim 1. Victim 1 stated that Childs had told her that he had to put Victim 3 "in her place." When Victim 1 asked what that meant, Childs told Victim 1 to "stop being stupid," and "she knew what that meant."

36. On Wednesday, February 7, 2018, Special Agent Jeff Berkley of the Wisconsin Department of Justice, Division of Criminal Investigation, conducted surveillance of the Geisha House. At approximately 8:42 a.m., a Cadillac registered to Childs and Campbell pulled into the parking lot. A female matching the general description of Victim 3 exited the front passenger seat, grabbed bags from the rear seat, and entered the side door of the building. On February 8, 2018, at approximately 1:38 am, SA Berkley observed the Cadillac return to the Geisha House. At 2 a.m., a female exited the Geisha house with bags, walked to Cadillac, and got into the front passenger seat.

37. In February 2018, case agents obtained authorization from United States District Judge Joseph P. Stadtmueller to intercept certain phone calls and text messages. This resulted in case agents obtaining recordings of calls in which Childs discussed Victim 3. For example, on February 9, 2018, at 10:47 a.m., Childs had the following interaction with Victim 1:

Victim 1: I'm guessing that [Victim 3] gives you everything?

Childs: Oh no questions; [Victim 3]… religiously. So I'm like okay, she likes the spot in Madison; you know what I'm saying? She doesn't want to leave. Like, now we talking last night, like before I picked her up and she doesn't want to go to Arizona now…to the Ranch.

Victim 1: Huh, really?

Childs: Yeah, she'd rather just stay at the Geisha House. I'm like when you break it down, when you think about it like that… You have… you fuckin' in 100, 200 bucks at the Geisha House. You're not doing that in Madison, I mean Vegas.

Victim 1: Right.

Childs: In Vegas, you're not giving away pussy for 100, 200 bucks.

Victim 1: No, not at all.

Childs: Anyway, you're giving away pussy out there…it's sometimes thousands.

Victim 1: Yep.

Childs: And even if the muthafucka pay a thousand just to fuck, you still get $500 of that.

Victim 1: Right, and it's not like it's a long time either.

Childs: Yeah, and like, she worked a double. She did, like, 13 programs on Wednesday, and that's cool, but that was a double. I mean, like, you fucked 13 people that day. You maybe sucked some, but for the most … 13. If you do 13 programs out at, you get 13 rooms out at the fucking Vegas, you get (unintelligible).

Victim 1: You're looking at 10 Gs.

38. The following is a transcribed excerpt of a call between Childs and Victim 1 on February 15, 2018, at 6:31 p.m.:

> Childs: The problem was…in the beginning [Victim 3] was at the Hardware Store, and [Campbell] was like, you need to put her out there by me 'cause there's a lot more money out there by me. And I'm like I can't keep an eye on her out there but [Campbell] kept pushing the issue and pushing the issue. I'm like, dude, get the fuck outta here man. Fine, it is a lot more money out there … so she goes out there and these bitches started getting up in her business…like [the owner of the Geisha House] was all up in her fucking business. Started talking mad shit to her.

F. Information learned following Childs' arrest.

39. On March 29, 2018, case agents arrested Childs and executed a search warrant for the residence he shares with Campbell. When reviewing Childs' phone, case agents confirmed that his Apple ID was **holidatstyle43@yahoo.com**.

40. On April 6, 2018, the FBI sent a preservation request to Apple related to the Apple ID **holidatstyle43@yahoo.com**.

41. When case agents arrested Childs, Campbell was in the Bahamas. On March 31, 2018, in connection with her departure from the Bahamas, the United States Customs & Border Protection Agency (CBP) reviewed Campbell's phone pursuant to their border search authority. Campbell was carrying an iPhone assigned telephone number **(262) 388-7485** (IMEI No. 359461081176969). I have confirmed that Verizon is the service provider for this phone. CBP also noted that the Apple ID and iCloud account linked to this phone belonged to Childs.

42. When looking at Campbell's iPhone, CBP Officers noted a text from Campbell to Childs on January 20, 2018. In the text, Campbell described the "programs" (prostitution dates) she was performing at the Geisha House:

> Hey sorry I haven't had a chance to text you.. been talking to [the owner of the Geisha House] and switching my schedule around… I will

> text you after I have a program… so far I have had 2… the first one was a basic 40 minutes… a basic program is where I only take my top off and give them a massage then a handy j… my second was a full program for an hour…. Full program is supposed to mean everything but a lot of guys don't make it past a Bj… this guy did for only a second. I will text you 1 for basic, 2 for Bj and 3 for full…. I will do this through out the day so that I don't have to talk about work at home… I will delete these messages and ask that you do the same…

43. CBP Officers also noted a text conversation between Campbell and Abigail Hageny. I am aware that Hageny is married to Mike Siegel, an owner of the Hardware Store strip club. Although the conversation is undated, it appears to relate to Childs and Victim 3's encounter with Hartford police officers as described in Paragraph 33 above. In the exchange, Campbell and Hageny discuss whether Victim 1 had called the police on Childs. Campbell states that she warned Childs "to get his ass out of town."

44. Since his arrest, Childs has been housed at the Dodge County Detention Facility. While detained, Childs frequently has called **(262) 388-7485**. Here are examples of his recent calls to Campbell's iPhone:

a. During a call at 2:59 pm on April 2, 2018, Campbell advised that she had seen Victim 1 and "wanted to go fucking kill her." Campbell stated that the owner of the Geisha House will not let her work due to the publicity from Childs' arrest.

b. During a call at 3:39 pm on April 2, 2018, Childs told Campbell that he had been arrested in Hartford, taken to court in Milwaukee, and then transported to jail "way out by Silk in Juneau." Childs joked that he could have driven "a bitch out here" to work at Silk, a strip club now owned by the owners of the Hardware Store.

c. During a call at 9:26 am on April 3, 2018, Campbell advised that agents did not take Childs' Apple watch, which was ringing.

d. During a call at 6:28 pm on April 3, 2018, Campbell advised that she had publicly identified Victim 1 on Facebook. In the call, Childs asked if his Apple watch had received any calls.

e. During a call at 12:43 pm on April 4, 2018, Childs explained that one of the victims in the criminal complaint was working with Campbell at the Geisha House. Childs also indicated that Victim 1 did in fact insert a curling iron, brush, and knitting needles in her vagina as described in the complaint but had done so voluntarily.

f. During a call at 7:57 pm on April 4, 2018, Campbell lamented that her work at the Chicken Ranch and Geisha House was now public. Childs advised Campbell that if she married him, she would not have to testify against him.

45. On April 6, 2018, the FBI also sent a preservation letter to Verizon for all records related to **(262) 388-7485**.

G. Information regarding Apple.

46. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system. Apple also produces the Apple watch, which can be synced to an iPhone via an Apple ID or iCloud account.

47. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be used through numerous iCloud-connected services and can store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage

images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share images and videos with other Apple subscribers.

e. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices.

f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System networks, and Bluetooth, to determine a user's approximate location.

g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers.

48. Apple services are accessed through an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism. In this case, it appears that Childs' Apple ID was linked to multiple iPhones (including Campbell's) and to his Apple watch.

49. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID.

50. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information. The user may also provide means of payment for products offered by Apple. The subscriber information

and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account, the methods used to connect to and utilize the account, the Internet Protocol ("IP") address used to register and access the account, and other log files that reflect usage of the account.

51. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

52. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be

captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service.

53. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud. Some of this data is stored on Apple's servers in an encrypted form but can be decrypted by Apple.

54. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. For example, stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity. In fact, in this case, Childs, Campbell, and others have communicated via text message and phone calls to further sex trafficking and unlawful prostitution activity. In addition, the stored communications and electronic data could

help identify additional victims of human trafficking and could provide evidence of the types of "punishment" photographs and videos described by Victim 1.

55. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

56. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

57. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store may reveal services used to communicate with victims and co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators, victims, and instrumentalities of the crimes under investigation.

H. Information from Verizon.

58. I am aware that Verizon provides cellular telephone access to the general public, and that stored electronic communications, including retrieved and unretrieved voicemail, text, and multimedia messages for Verizon subscribers, may be located on the computers of Verizon. Further, I am aware that computers located at Verizon contain information and other stored electronic communications belonging to unrelated third parties.

59. Wireless phone providers often provide their subscribers with voicemail services. In general, a provider will store voicemail messages on behalf of a particular subscriber until the subscriber deletes the voicemail. If the subscriber does not delete the message, the message may remain in the system of Verizon for weeks or months.

60. Among the services commonly offered by wireless phone providers is the capacity to send SMS or MMS messages (photos, audio, or video) from one subscriber's phone or wireless device to another phone or wireless device via one or more wireless providers. Based on my knowledge and experience, I know that stored electronic communications, including SMS and MMS messages that have been sent or received by subscribers, are stored by Verizon for short periods incident to and following their transmission. In addition, providers occasionally retain printouts from original storage of text messages for a particular subscriber's account.

61. Wireless phone providers typically retain certain transactional information about the use of each telephone, voicemail, and text-messaging account on their systems. This information can include log files and messaging logs showing all activity on the account, such as local and long distance telephone connection records, records of session times and durations, lists of all incoming and outgoing telephone numbers or e-mail addresses associated with particular telephone calls, voicemail messages, and text or multimedia messages. Providers may

also have information about the dates, times, and methods of connecting associated with every communication in which a particular cellular device was involved.

62. Wireless providers may also retain text-messaging logs that include specific information about text and multimedia messages sent or received. A provider may also retain information about which cellular handset or device was associated with the account when the messages were sent or received. The provider could have this information because each cellular device has one or more unique identifiers embedded inside it. Depending upon the network and device, the embedded identifiers for a cellular device could take several different forms, including an Electronic Serial Number ("ESN"), a Mobile Electronic Identity Number ("MEIN"), a Mobile Identification Number ("MIN"), a Subscriber Identity Module ("SIM"), an International Mobile Subscriber Identifier ("IMSI"), or an International Mobile Station Equipment Identity ("IMEI"). When a cellular device connects to a cellular antenna or tower, it reveals its embedded unique identifiers to the antenna or tower in order to obtain service, and the cellular antenna or tower records those identifiers as a matter of course.

63. Many wireless providers retain information about the location in which a particular communication was transmitted or received. This information can include data about which cell towers received a radio signal from the cellular device and thereby transmitted or received the communication in question.

64. Wireless providers also maintain business records and subscriber information. This could include names and addresses, the address to which any equipment was shipped, the date on which the account was opened, the length and types of service utilized, the ESN or other unique identifier for the cellular device associated with the account, and all telephone numbers and other identifiers associated with the account. In addition, wireless providers typically retain

billing records for each account, which may show all billable calls (including outgoing digits dialed). The providers may also have payment information for the account, including the means and source of payment (including any credit card or bank account number).

65. In some cases, subscribers may communicate directly with a wireless provider about issues relating to the account. Wireless providers typically retain records about such communications.

66. Like the Apple ID / iCloud information described above, information stored at the wireless provider, including that described above, may provide evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation. In my training and experience, the data pertaining to a particular cellular device that is retained by a wireless provider can show how and when the cellular device and associated cellular service were accessed or used. Such "timeline" information allows investigators to understand the chronological context of cellular device usage, account access, and events relating to the crime under investigation. Additionally, information stored by the wireless provider may indicate the geographic location of the cellular device and user at a particular time (e.g., historic cell-site location information; location integrated into an image or video sent via text message to include both metadata and the physical location displayed in an image or video).

IV. Conclusion.

67. Based on the information set forth above, I submit that probable cause supports the issuance of the requested search warrants for information retained by Apple and Verizon.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **holidatstyle43@yahoo.com** (the "account") that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information is within the possession, custody, or control of Apple, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for the account listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

d. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iCloud Tabs, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

e. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs, iCloud logs, messaging and query logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers);

f. All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;

g. All records pertaining to the types of service used;

h. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

i. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

II. Information to be seized by the government.

All information described above in Section I that constitutes evidence or instrumentalities of violations of Title 18, United States Code, Section 1591 (sex trafficking by force, fraud, and coercion), and Title 18, United States Code, Section 1952 (use of a facility in interstate commerce to carry on unlawful activity involving prostitution), involving Christopher L. Childs and Jennifer E. Campbell, since January 1, 2009, including, for the account listed on Attachment A, information pertaining to the following matters:

a. Communications in any form between Childs, Campbell, strip club / brothel owners and employees, victims, other pimps, and/or prostitution customers;

b. Use of third-party apps and websites, such as Facebook, related to the offenses under investigation;

c. All videos, photographs, and images involving or documenting contact between Childs or Campbell and strip club / brothel owners and employees, victims, other pimps, and/or prostitution customers

d. The identity of the persons who created and who have used the Apple ID, including records that help reveal the whereabouts of such persons when using the Apple ID;

e. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

f. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

g. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and

h. Evidence that may identify any co-conspirators, aiders and abettors, or victims including records that help reveal their whereabouts.